Secret Key Exchange and Authentication via Randomized Spatial Modulation and Phase Shifting

DOI:
10.1109/TVT.2017.2764388

Document Version
Accepted author manuscript

Secret Key Exchange and Authentication via Randomized Spatial Modulation and Phase Shifting

Hasan Taha, *Student Member, IEEE,* Emad Alsusa, *Senior Member, IEEE*

***Abstract*—Advances in physical layer security techniques have increasingly demonstrated their potential to replace security functionalities that are traditionally included in the upper layers of the OSI model. This has made it possible for devices with limited layer structures or/and restricted hardware components to offer security measures. In this paper, we consider Spatial Modulation (SM) systems and propose a unique physical layer technique that uses a random constellation mapping criterion for secret key exchange. The principle idea here is to exploit the inherent symbol-antenna mapping feature of the SM technique to encode the secret key. Specifically, a random phase shift is imposed on each of the modulated symbols using a channel driven approach to uniquely authenticate the transmitted key bits or/and the encrypted confidential data. The results demonstrate that the proposed technique is superior to benchmark techniques in terms of computational complexity and key bit error rate. It will also be shown that the proposed technique offers greater flexibility in terms of the authentication process preference which is normally unattainable in most of the key exchange proposed techniques.**

***Index Terms*—Authentication, MIMO systems, physical layer security, secret key exchange, spatial modulation.**

I. Introduction

THE fast growth in both wired and wireless devices as well as network topologies and functionalities fostered a steady progress in advancing security protocols. The Open Systems Interconnection model (OSI) has a security ensemble that involves encryption, authentication and message digestion. The implementation of security algorithms in all layers within the protocol stack can be done to gain more secure connection but at the expense of increased complexity and power consumption. Enhancing security measures is particularly important in wireless communications which suffers from an additional secrecy vulnerability due to its open air channel that exposes it to malicious access and adversary attacks [1]. Moreover, many emerging wireless devices tend to have limited capabilities with limited access to a central management unit in their network. One example of such a network is the Intelligent Transport System (ITS) which is designed to increase road safety and comfort by facilitating the exchange of traffic information, such as road queueing conditions, traffic speed, traffic signs, and emergency vehicles warnings, etc. Therefore, such a link has to be equipped with robust security and privacy mechanism. In this paper, we aim to provide this type of network with a method for secret key management and authentication combined, as opposed to many of the schemes found in the literature which consider secret key exchange and authentication separately.

The authors are with the School of Electrical and Electronic Engineering, University of Manchester, Manchester M13 9PL, U.K. (e-mail: hasan.taha@manchester.ac.uk; emad.alsusa@manchester.ac.uk).

A. Related Work

1) Secret Key Management: Research on physical layer security was motivated by the early information theoretic security approaches to thwart illegitimate reception or intrusion of the exchanged data [2]. The early information theoretic work studied keyless cryptography, also known as the unshared secret key cryptography, with the objective to increase the secrecy capacity using a wiretap channel [3], [4]. Inspired by this work, researchers proposed to inject artificial noise, jamming, or beamforming techniques into the intruder's channel to make the confidential information hard to detect [5]-[7]. These techniques however usually come with increased complexity making them less desirable than shared secret key cryptography. A basic methodology for establishing secret keys is by extracting the shared randomness from the channel state information (CSI) which is highly correlated in time-division duplex (TDD) channels, due to channel reciprocity [8]. Hence, the channel offers a highly correlated random distribution between two communicating nodes operating at the same frequency. In order to use the estimated random values as a shared secret key, many methods proposed to use a quantization technique of the channel gain coefficients such as its magnitude, phase, or both [9]-[12]. Recently, some techniques were proposed to increase the secret key length and lower the key error rate (KER) in multiple-input multiple output (MIMO) systems [13]-[15]. In vehicular networks, the authors in [16] proposed two methods for secret key generation that utilize differential and channel-hopping algorithms, but such algorithms strongly rely on the reciprocity of the channel and hence will generate correlated secret bit sequences that may degrade the randomness of the secret bits and secrecy level in low mobility. Other vehicular communication protocols proposed exchanging the secret key using a third parity for authentication, [17], which may not always be possible since the presence of a central management may be limited to a road side unit (RSU) as shown in Fig. 1.

2) Message Authentication: The other significant part of the security aspects is message authentication which offers integrity and eliminates, or at least reduces, the repudiation. Basically, the authentication process is used to verify whether the received message was generated from the legitimate transmitter or not. Commonly, two types of coding are considered in the lower layers of the OSI model as an authentication service: 1) Message Integrity Codes (MICs), and 2) Message Authentication Codes (MACs). The MICs result as a function of the input message such that it will generate the same code for the same given message. Conversely, the latter MACs use shared secrets and will not generate the same code only

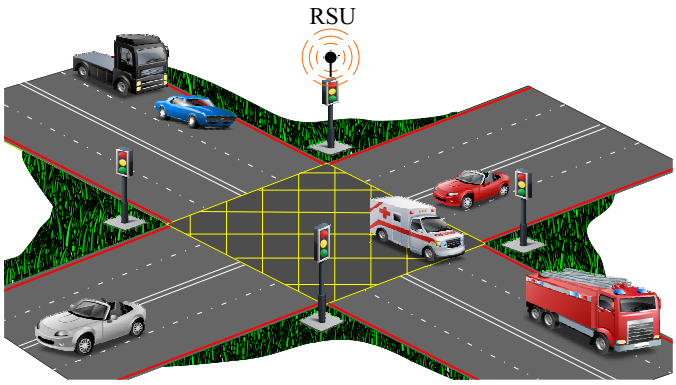

Fig. 1. Road Side Communications

if the same secret key and the same initialization vector were used. As the MACs are generated as a function of the transmitted message, the receiver can detect the source of the message by computing the MAC of the received message and comparing it to the transmitted MAC. Both MICs and MACs share an advantage of being transmitted with the same quality as the data bits, but result in a loss of throughput and the shared secret problem will still exist in the MACs. It is worth mentioning that the acronym "MAC" also stands for another type of authentication that matches the Media Access Control address to authenticate the received packets. This type of authentication is considered weak since a simple software masquerade attack can be done by the adversary.

Many researchers proposed the use of physical layer information to enhance the wireless authentication process. Specifically, the receiver compares the correlation of the information between two consecutive messages, if it falls to high correlation with the first received message thereafter it is more likely to be generated from the same source. Before indulging more in related works in this area it is worth defining two types of authentication errors: 1) False Alarm (FA) which happens when a message from a legitimate transmitter is identified as non-authentic, and 2) Missed Detection (MD) which occurs when an attacker succeeds in impersonating the legitimate transmitter and the received malicious message is authentic.

In [18], the authors proposed a generalized likelihood ratio test (GLRT) for authenticating the sequential packets but this is not always applicable in practice due to the cumbersome computational complexity of such a technique and the requirement of prior knowledge of channel parameters. Furthermore, the authors offered a simplified version of the GLRT method by assuming a small effective amount of channel estimation errors and variance which is only applicable when the adversary has lower signal-to-noise ratio (SNR) than the legitimate receiver when both are connected to the same transmitter. Another GLRT based test of the power spectral density comparison proposed to evaluate the authentication of the subsequent CSI measurements in [19]. In time-variant environments, a hypothesis test based on the channel frequency response (CFR) was proposed in [20]. As an alternative method, in [21], the authors used a logarithmic likelihood ratio test (LLRT) to authenticate a message by computing the difference between two consecutive quantized channel impulse responses (CIR). Moreover, in [22], the authors proposed to trace the received signal strength (RSS) measurement. These types of authentication face serious challenges under mobile conditions since they rely on exploiting the difference between two packets with a time gap that may be greater than the coherence time and hence a rapid decorrelation in the spatial properties are expected to generate multiple false alarms. The other drawback is their reliance on a threshold value to evaluate the authentication process with a trade-off between false alarms and missed detections.

B. Main Contribution

Spatial modulation (SM) is a multiple antenna concept designed to enhance spectral efficiency with a low complex implementation. In the conventional SM technique, the multiplexing gain is achieved by mapping information bits into two carriers, the modulation symbol and the index of the transmitting antenna [23]. In [24], the authors proposed a fixed phase shift for the SM symbols-antenna pair to improve performance and transmit diversity in MISO systems. Moreover, the authors proposed to increase the single radio frequency SM transmit diversity gains and improve power efficiency in SM-MIMO scenarios in [25], [26].

In this paper, inspired by previous studies we propose a scheme that consists of two components. The first one is to solve the problem of the secret key exchange in order to randomize the secret key bits sequences in low mobility conditions and to utilize a robust exchange method in the low SNR environments. We manipulate the conventional SM technique and propose a Random Spatial Modulation (RSM) approach to randomize the pattern of the constellation mapping of the modulated symbols without compromising the system's bit error rate performance. In this case however, the transmitter and the receiver have to agree on the type of mapping which can exploit the multiple antenna channel gains by assigning each antenna a specific constellation depending on its channel gain with respect to the antennas at the legitimate receiver of the secret key. The performance of this technique, on the basis of the KER, is compared to published benchmark techniques, such as in [12], [15], [27], and [28]. The KER comparison shows a superior performance compared to these benchmarks. Furthermore, it will be shown that the proposed technique only requires relatively low complexity for a wide range of SNR values. Moreover, it will be demonstrated that the correlation to a nearby passive eavesdropper is relatively low to mislead the secret key passive attack.

The second part of the contribution concerns designing an authentication technique with low complexity to relax the user's displacement between two packets to make the proposed algorithm suitable for both time invariant and variant systems. We propose to use a Random Phase Shift (RPS) approach to divide the constellation region of the complex symbols into multiple sub-regions equal to the number of antennas at the transmitter and with a significant variable minimum distance to adjacent symbols. The distribution of symbols on these multiple sub-region is related to the channel gain of each

transmit-receive link. The receiver now detects the transmitted symbol in a specific region, whether it belongs to the assigned antenna or not, and if so then the symbol packet is considered authentic. Particularly, it will be shown that the false alarm and missed detection rates are independent in the presence of an active eavesdropper which makes the threshold value no longer necessary.

C. Organization and Notation

The rest of the paper is organized as follows. Section II introduces the system model. In Section III, we describe the proposed algorithms, the secret key exchange and the authentication process. Theoretical analyses are presented in Section IV and detailed in the appendixes. The simulation results, discussion and the generalization of the proposed method are provided in Section V. Conclusions are drawn in Section VI.

The following notations are used in this paper. Lower bold faces and upper case symbols are used to denote vectors and matrices, respectively. The operators $(\cdot)^{-1}$, $(\cdot)^{\star}$, $(\cdot)^{T}$ and $(\cdot)^{\dagger}$ denote the matrix inversion, matrix conjugate, matrix transpose and matrix hermitian, respectively. Finally, $(\cdot)_b$ represents a binary value assignment.

II. System Model

A. Basics of Spatial Modulation

Let us consider a generic MIMO system of size $N_R \times N_T$, where N_R and N_T represent the number of antennas at the receiver and the transmitter, respectively. Assume a typical SM scheme where the transmitter can send two types of data, 1) T symbols to identify the index of the antenna used at the transmitter, and 2) M modulated information symbol constellation using a specific digital modulation scheme such as M-ary phase shift keying (MPSK). Traditionally, the first type of symbols are known as the spatial constellation diagram, whilst the latter symbols are called the signal constellation diagram, [29]. Fig. 2 shows a basic concept of the two constellation diagrams in the space of the complex planes.

In single carrier systems, the transmitter generates a bit stream of data to a dedicated user and divides each block of bits into two sub-blocks with $\log_2(T)$ and $\log_2(M)$ bits each for spatial and signal constellation diagram, respectively. The first sub-block is used to switch-on the corresponding antenna while the rest of the antennas are kept off during the transmission time interval. For example in Fig. 2, suppose that a Quadrature-PSK modulation is used with $N_T = 4$, a binary block of $(0111)_b$ is used to send $(11)_b$ complex symbol from an antenna of $(01)_b$ index with the help of a SM-Mapper which guides the whole transmission scheduling and processing. In multicarrier systems, assuming an orthogonal frequency division multiplexing (OFDM) system with R subcarriers, the received Rayleigh flat fading signal can be expressed as

$$\mathbf{y} = \mathbf{H}\mathbf{x} + \mathbf{n}, \tag{1}$$

where $\mathbf{H}$ is an $N_R \times N_T$ matrix with independent and identically distributed (i.i.d) elements with $h_{r,t}$ being the t-th transmit antenna channel towards the r-th receive antenna

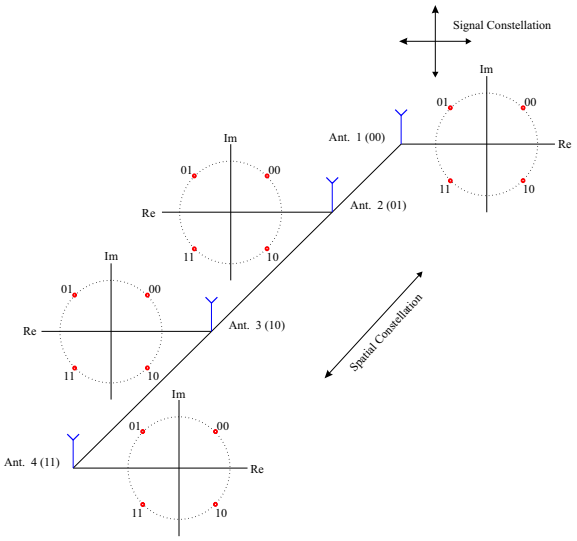

Fig. 2. Spatial Modulation space.

which is independently drawn from $\mathcal{CN}(0,1)$. $\mathbf{x}$ is the modulated symbols vector and $\mathbf{n}$ is the noise vector of length N_R with the i.i.d entries according to $\mathcal{CN}(0, N_0)$. This model gives a wide degree of freedom since only a single antenna is activated on a single subcarrier, we can represent the case of multiple symbols on different orthogonal subcarriers and assume the effect of the inter-symbol interference is neglected at this instant. At the receiver, assume a bandpass filter and a SM-Demapper are used to indicate each antenna signal with respect to the signals transmitted by the other antennas and subcarriers by solving a $T \times M \times R$ detection problem which estimates the index of the transmit antenna that is not idle on a specific subcarrier as well as the complex symbols transmitted over this communication channel.

B. Adversary Model

Assume the same terminology adopted by the security community which defines three parties: Alice, Bob and Eve. Through out this paper, we assume that Alice (as a transmitter) communicates with Bob (as a receiver) in the presence of (an eavesdropper referred to as) Eve, each equipped with multiple antennas of size N_A, N_B and N_E, respectively. Since Alice serves as a transmitter then

$$N_A \quad \geq \quad N_B. \tag{2}$$

Fig. 3 shows the former two communicating parties where Eve has a position close to one of them in order to seek the best practice of an adversary modelling that is independent of the SNR towards the transmitter and/or the receiver. With this in mind, our goal is to provide privacy (secret key establishment and authentication) despite the presence of an eavesdropper. The opponent of this secure communication will possibly serve two common types of attacks as:

1) Passive Attack: In this type of attack Eve aims to find leakage in the secret key bits stream in order to apply a brute-force attack on the encrypted messages after the secret key setup. Assume Eve is acting as a passive illegitimate

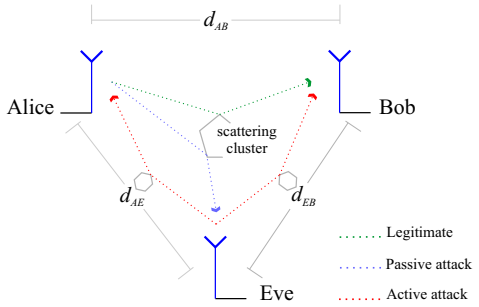

Fig. 3. Adversary model schematic where d is the separating distance.

receiver who listens to the whole secret key negotiation and reconstructs her channel into a correlated version with the channel established between Alice and Bob ($\mathbf{H}_{AB}$) as, [30], [31],

$$\mathbf{H}_{AE} = \rho \mathbf{H}_{AB} + \sqrt{1-\rho^2}\mathbf{H}_{i.i.d}, \tag{3}$$

and,

$$N_E = N_B, \tag{4}$$

where $\mathbf{H}_{AE}$ is the channel between Alice and Eve has correlation with $\mathbf{H}_{AB}$ in a wide sense with $0 \leq \rho \leq 1$. $\mathbf{H}_{i.i.d}$ represents an i.i.d. Rayleigh fading channel and it is totally uncorrelated with $\mathbf{H}_{AB}$. Thus, the received signal in (1) can be expressed as

$$\mathbf{y}_B = \mathbf{H}_{AB}\mathbf{x} + \mathbf{n}_B, \tag{5}$$
$$\mathbf{y}_E = \mathbf{H}_{AE}\mathbf{x} + \mathbf{n}_E. \tag{6}$$

2) Active Attack: Eve's main objective here is to insert masquerade secret key bits into the legitimate communication channel between Alice and Bob in order to:

- disturb the secret key exchange session as a denial-of-service attack and/or,
- setup a malicious key as a man-in-the-middle attack scenario.

The malicious adversary will serve in an active role trying to inject vague information into the communication medium towards Bob. Bob detection process in this case has to authenticate the received signals and detect the original source whether it comes from a legitimate Alice or other spoofing signals by applying an authentication process. Meanwhile, Eve is trying to impersonate Alice and will try to reconstruct her channel towards Bob as a correlated version of Alice-Bob channel. Hence, the correlated version of the channel between Eve and Bob is

$$\mathbf{H}_{EB} = \rho \mathbf{H}_{AB} + \sqrt{1-\rho^2}\mathbf{H}_{i.i.d}. \tag{7}$$

III. The Proposed Algorithm

In this section we provide a detailed description of the proposed RSM and RPS algorithms.

A. The RSM Algorithm

The idea here is to rotate the constellation mapping with a fixed phase shift; to be more specific, we use different mapping probabilities in a similar manor as in [32], in which the purpose was to improve diversity over fading channels. To clarify the algorithm for example in the case of SM-QPSK with four transmit antennas we use different constellation mapping as shown in Fig. 4. In other case of higher multiple antenna orders, we propose to use other constellation mapping that can be produced by flipping the symbol's assignment with respect to the imaginary and/or the real axis. To clarify further, let us consider the constellation mapping set

$$C^{Public} = \{c_{Ant.1}, c_{Ant.2}, c_{Ant.3}, \ldots, c_{Ant.T}\}, \tag{8}$$

which includes the publicly known constellation distributions for each of the allocated antennas at the transmitter. Basically, to send secret key bits over a public channel we propose to apply, at the transmitter and the receiver, a new indexing for the constellation maps provided in the public set where the new order is based on the antenna channel gain between the legitimate transmitter and receiver since the antenna channel gain is reciprocal in TDD systems. Thus, the new private set is

$$C^{Private} = \{\bar{c}_{Ant.1}, \bar{c}_{Ant.2}, \bar{c}_{Ant.3}, \ldots, \bar{c}_{Ant.T}\}, \tag{9}$$

where

$$\bar{c}_{Ant.1} \triangleq \underset{1<i\leq T}{\text{argmax}} \left|h_{Bob,\ Ant_i}\right|, \tag{10}$$
$$\bar{c}_{Ant.T} \triangleq \underset{1<i\leq T}{\text{argmin}} \left|h_{Bob,\ Ant_i}\right|. \tag{11}$$

where $\bar{c}_{Ant.T}$, is the private constellation pattern at the T-th antenna on the downlink channel from Alice to Bob, $h_{Bob,\ Ant_i}$, and h is the one-to-one antenna channel vector. Similarly, the T-th antenna at Eve's side will have a private mapping as $\bar{c}_{Ant.T} \triangleq \underset{1<i\leq T}{\text{argmin}} \left|h_{Eve,\ Ant_i}\right|$.

B. The RPS Algorithm

We propose the RPS algorithm to provide authentication in the device-to-device (D2D) scenario without the need for a third trusted party for central authentication management, as the scenario shown earlier in Fig. 1.

In this algorithm, assume a modulated symbols vector, $\mathbf{s}$, before the transmission takes place as

$$\mathbf{s} = \left[s_{0,Ant.1},\ s_{1,Ant.2}, \ldots,\ s_{T-1,Ant.T}\right], \tag{12}$$

where s is the symbol generated from a block of the secret key bits, k. Firstly, we divide the M-ary regions into P (where $P = T \times R$) sub-regions each of a total fixed window width (W) as for 4 transmit antennas

$$W = 2\left(\theta_1 + (\theta_1 - 2\theta_4)\right) + 2\left(\theta_2 + (\theta_2 - 2\theta_3)\right), \tag{13}$$

for each symbol as shown in Fig. 5. Then we insert a different phase shift to each symbol transmitted on a different transmit

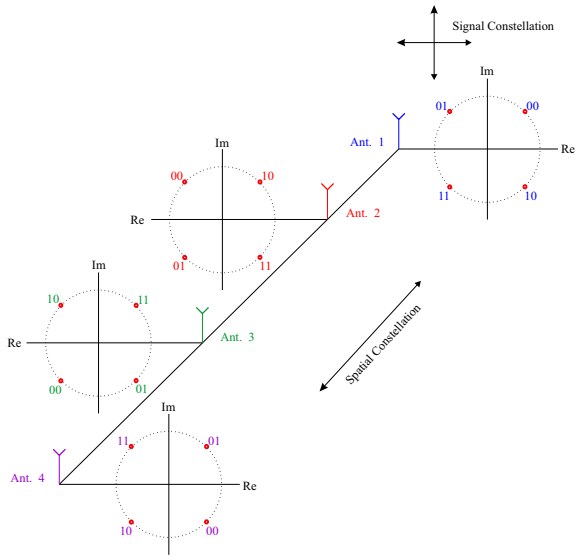

Fig. 4. The RSM variable constellation mapping with $T = 4$ antennas and QPSK modulation. It can be also referred as a constellation rotation with 90°.

antennas and the legitimate modulated symbols set for a single time burst is

$$\mathbf{x} = \left[s_0 e^{j\theta_1}, s_1 e^{j\theta_2}, s_2 e^{j\theta_3}, \ldots, s_{T-1} e^{j\theta_T}\right], \qquad (14)$$

where θ is the phase shift value of the corresponding antenna.

At this stage the objective of this algorithm is to 1) gain the advantage of this inserted phase in the authentication process and 2) hinder the adversary from reconstructing the distribution of the sub-regions especially at high SNR values of the downlink where Eve gains the advantage of a low noise power signal. Hence, we propose to adapt the shape of the sub-regions distribution with variable width as a function of the communication link between the transmitter and the legitimate receiver antennas as depicted in Fig. 5. Thus,

- We design variable sub-windows, w, width for each antenna for the same symbol as

$$W = w_1 + w_2 + \cdots + w_T. \qquad (15)$$

- Antennas with higher transmit-receive link gain will have narrower sub-windows. For Antenna gains

$$G_1 > G_2 > \cdots > G_T, \qquad (16)$$

will result in

$$w_1 < w_2 < \cdots < w_T. \qquad (17)$$

- A space for the antennas with higher channel gains will be allocated at the edges and those with low gains will be positioned close to the centre of the conventional mapping in order to eliminate symbols transmitted on low channel gain antennas from interfering to each other at the receiver.
- The allocated spaces for antennas at the edges are reciprocal to the adjacent symbol in order to keep antenna's index detection probability as high as possible as proved later in Appendix B.

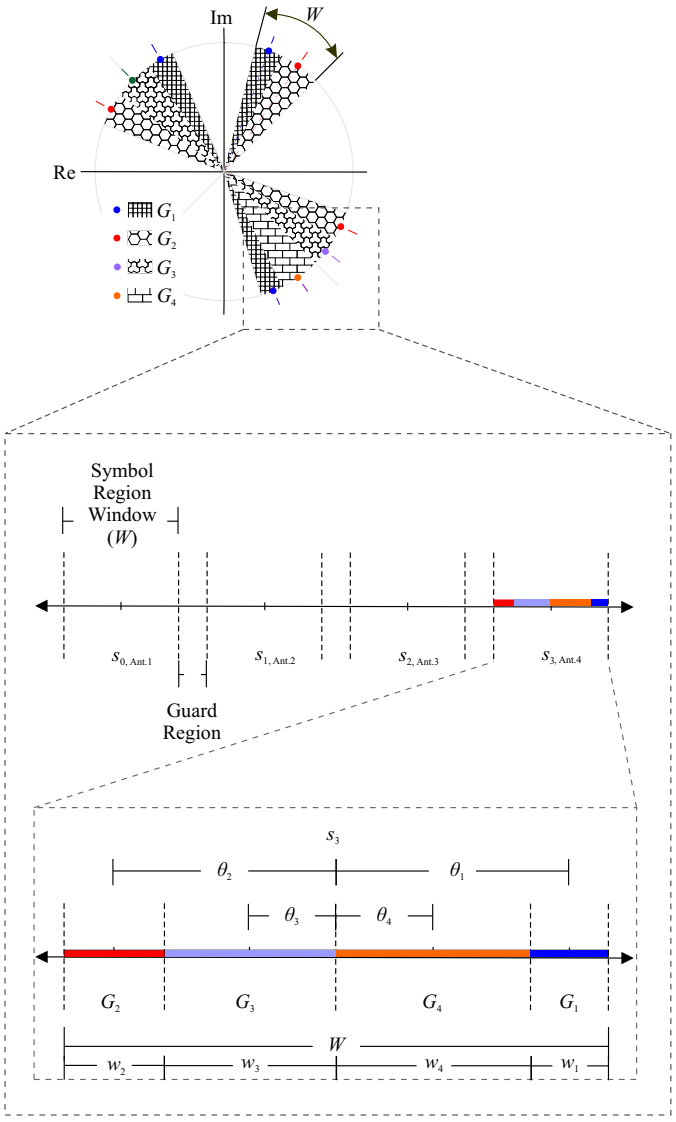

Fig. 5. The RPS sub-regions in variable sub-regions QPSK that depend on the antenna channel gains (G_1,..., G_T) where $G_1 > \ldots > G_T$.

In reality the inserted phase can be considered as a man-made phase noise; as a result it will divert the symbol from its traditional region which is susceptible to the noise at the receiver. Hence, the receiver calculates the minimum Euclidean distance of the private phase of the private mapping of the symbols relative to the received private phase using a maximum likelihood modular reduction method as

$$D_{\text{Euclidean},\hat{i}} = \underset{1 \le i \le T}{\text{argmin}} \left(\left| \text{mod}(\measuredangle \bar{\mathbf{x}}_i, \measuredangle \mathbf{s}_i) \right| \right). \qquad (18)$$

At this moment, both Alice and Bob have the same knowledge of the private antenna order and mapping, whereas Eve is left puzzled of this process. In practice, the intruder Eve is expected to seek a position to get a replicated version of the secret channel which can be realized in practice by moving towards the receiver, Bob, ($d_{AE} \gg d_{EB}$) and use its estimate

to masquerade Alice by sending her malicious key bits. It will be simulated later in this paper how the RPS algorithm is independent of Eve's position and her SNR values.

C. Secret Key Exchange and Authentication Algorithm

Here we summarize the secret key exchange between Alice and Bob, where Fig. 6 shows a schematic of the essential blocks (including the OFDM Fourier transform blocks, the IFFT/FFT, and the estimator of the channel state information (CSI) block) which can be outlined as follows:

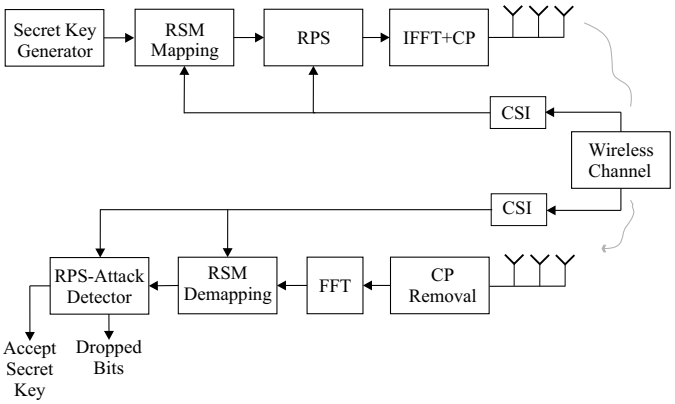

Fig. 6. Proposed RSM and RPS block diagram.

1) Alice generates random secret key bits of length k, and groups each M-bits, then maps it to a random transmitter using its corresponding constellation.
2) Bob retrieves the symbol by measuring which region in the constellation map it falls. Then, he also measures which sub-region the symbol belongs to.
3) If the symbol falls into the sub-region of the corresponding antenna then, Bob authenticates and accepts the symbol as part of the secret key.
4) Optionally, Bob transmits another sequence of secret key bits on the uplink using the above steps.
5) Privacy Amplification process: both Alice and Bob exchange their received key bits using a universal Hash function for private acknowledgement [1], [33]. The optimal decision of a low complexity Hash function is out of the scope of this paper and more details can be found in [33].

IV. Theoretical Analysis

The purpose of this section is to clarify an understanding of the signal processing that will maintain the security services, the secret key exchange and authentication.

A. Probability of Error Rates

Firstly, we will study the signal transmission performance and the effect of the proposed random phase insertion. Then, we will analyse the performance of the phase shifting on the receiver side and the recovery process error rate. Under the phase shift keying (PSK), the key bits and the active transmit antenna determines the phase of the carrier which earns its value from the constellation mapping set that is defined earlier in Section III-A. A QPSK signal can be two dimensional signal constellation with four regions of dibits. As shown in Fig. 4 the message bits are dependent of the transmitting antenna and correspond to four general phases $\frac{\pi}{4}$, $3\frac{\pi}{4}$, $5\frac{\pi}{4}$, and $7\frac{\pi}{4}$. The signal strength of these symbols are equal to the energy symbol, E_s. In general, the QPSK signal is given by

$$s_i(t) = \sqrt{\frac{2E_s}{T_s}} \cos\left(2\pi f_c t + \omega_i\right), \qquad i=1,2,3,4, \tag{19}$$

where

$$\omega_i = 2\frac{\pi}{4}(i-1), \qquad i = 1,2,3,4, \tag{20}$$

and

$$E_s = \int_0^{T_s} y_i(t)\, dt \tag{21}$$

Theorem 1. *Let us consider a given QPSK system with 1×2 MISO system and it is working under our proposed algorithms RSM and RPS, with an equal phase offset θ between the randomized symbols in single zone and a maximum window width $W = 2\theta_1 + 2\theta_2$, then the symbol error rate is*

$$P_s \simeq \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_1 - \sin\theta_2)\right) + \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_1 + \sin\theta_2)\right), \tag{22}$$

(23)

where,

$$\text{erfc}\,(x) = \frac{2}{\sqrt{\pi}}\int_x^{\infty} e^{-u^2} du. \tag{24}$$

Proof: The proof of Theorem 1 is shown in Appendix A. ■

Lemma 2. *Given the same system and algorithm in Theorem 1, the phase error rate of the shift detection is*

$$P_p \simeq \frac{1}{4}\left[\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_1)\right) + \text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_2)\right)\right] + \frac{1}{2}\left[\text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,(\sin\theta_1)\right) + \text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,(\sin\theta_2)\right)\right]. \tag{25}$$

(26)

Proof: The proof of Lemma 2 is shown in Appendix B. ■

Corollary 3. *A useful corollary to Lemma 2, for multiple antenna system with $N \geq 4$ transmit antennas, high values of ${}^{E_s}/_{2N_0}$ in dB, and variable phase shift θ and a maximum window width $W = 2\theta_1 + 2\theta_2$, then the phase error rate is*

$$\begin{aligned} P_p \simeq & \frac{1}{N}\left[\frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_1)\right)\right. \\ & + \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\theta_2)\right) \\ & + \text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,(\sin\theta_{N-1}+\sin\theta_N)\right) \\ & \left. + 2\sum_{i=1:i+2}^{N-1}\text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,\sin\,(\theta_i-\theta_{i+2})\right)\right]. \end{aligned} \tag{27}$$

B. Trade-off Factor Evaluation

In order to understand the system performance with the proposed algorithms, we plot the error rates both for the QPSK symbol and the phase shift detection in Fig. 7 and Fig. 8, respectively.

It is clear that the inserted phase will act as a man-made noise whereas the maximum window width has to be less than $\frac{\pi}{2}$. In the case of two transmit antenna QPSK system, the symbol detection sub-region is $\frac{\pi}{4}$ allowing a phase shift of $\pm\frac{\pi}{8}$. Mathematically, the first term in equation (22) , $(\cos\theta_1 - \sin\theta_2)$, is the most dominant part and will converge the error function to its maximum values as the phase shift (i.e. the window width, W) is increasing. In practice, this added phase will proportionally affect the performance of the SER and will degrade it as the phase angle increases, this is because the wider the distribution of the symbols the closer in the constellation diagram. Conversely, the phase error rate in equation (25) will depend on the last sinusoidal term where its performance will be enhanced with wider angles of phase shift since the Euclidean distances in-between the jointly distributed symbols of different antennas are spaced far apart. But this advantage in the phase error rate has to be gleaned carefully based on the SNR of the intermediate channel to compromise an acceptable performance of both the symbol and the phase detection processes. The optimal decision of setting the trade-off factor, the window width, will be decided based on the security available preferences between the targeted KER and the authentication priority level as shown in Fig. (9).

C. Mutual Information and Equivocation

The achievable mutual information in the direct channel quantization approach is identical to the jointly quantized random variables x and y, $I(x;y)$, [34], as

$$I_{\text{bits}} = I\left(\mathbf{H}_{\text{Alice-Bob}}; \mathbf{H}_{\text{Bob-Alice}}\right), \tag{28}$$

where $\mathbf{H}_{\text{Alice-Bob}}$ is the downlink channel matrix between Alice and Bob and $\mathbf{H}_{\text{Alice-Bob}} = \left(\mathbf{H}_{\text{Bob-Alice}}\right)^T$ for TDD systems. In our case, we will consider the mutual secret information as

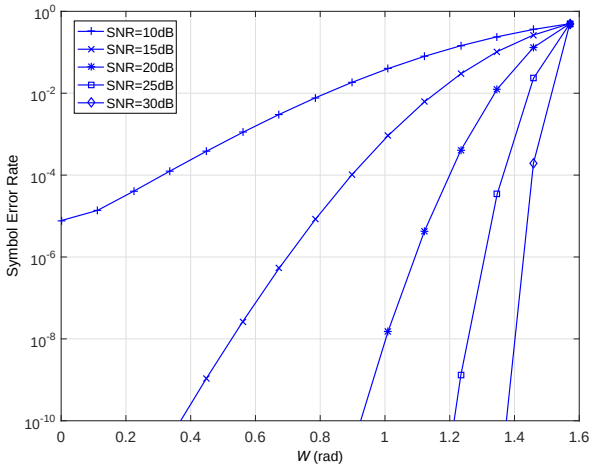

Fig. 7. QPSK performance under different window sizes, W in radians.

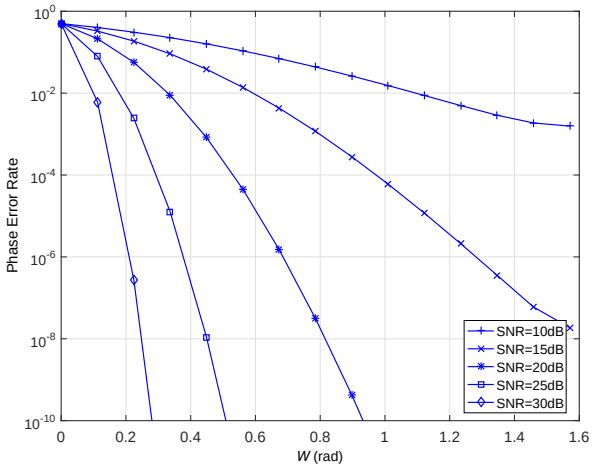

Fig. 8. QPSK performance under different window sizes, W in radians.

$$I_{\text{secret}} = I\left(h_{\text{ALice-Bob}}; h_{\text{Bob-ALice}} \mid h_{\text{Alice-Eve}}, h_{\text{Bob-Eve}}\right), \tag{29}$$

where h is the point-to-point established channel in the downlink/uplink channel vector.

The upper bound or the maximum mutual secret information, $I_{\text{secret}} \leq I_{\text{bits}}$, is achievable when Eve's displacement from both ALice and Bob is longer than half the operating wavelength [14]. In this case, all the secret bits are secure since the corresponding adversary passive channels as

$$h_{\text{ALice-Bob}}, h_{\text{Bob-ALice}} \perp h_{\text{Alice-Eve}}, h_{\text{Bob-Eve}}. \tag{30}$$

The lower bound happens when Eve is closer to Alice or Bob and in a wide sense stationary to the respect of one of them. In vehicular communication systems, the case of having both the base station and the users stationary is not applicable for a long period of time especially when the scattering environment is changing during less than the coherence time.

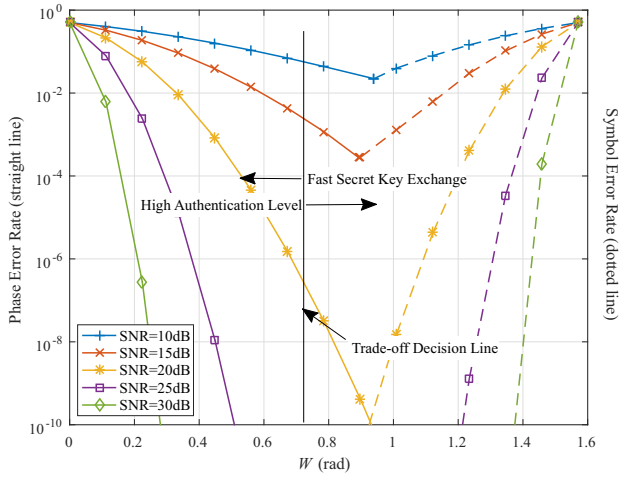

Fig. 9. SER and PER trade-off strategy.

Thus, only one channel will exist, $h_{\text{Alice-Eve}}$ or $h_{\text{Bob-Eve}}$, since the uplink and the downlink are not synchronized. Hence equation (29) can be rewritten considering our proposed additive random phase shift,

$$I_{\text{secret}} = I\left(h_{\text{ALice-Bob}}e^{j\theta_i}; h_{\text{Bob-ALice}}e^{j\theta_j} \mid h_{\text{Alice-Eve}}e^{j\theta_k}\right). \tag{31}$$

where (i, j, and k) are the additive phase indexes. The secret key bits can be simplified as the equivocation of the downlink channel, $\text{h}(h_{\text{ALice-Bob}} \mid h_{\text{Alice-Eve}})$, multiplexed with the uplink channel, $\text{h}(h_{\text{Bob-Alice}} \mid h_{\text{Alice-Eve}})$, and the joint probability of Alice, Bob, and Eve as

$$\begin{aligned} I_{\text{secret}} &= \text{h}(h_{\text{ALice-Bob}}e^{j\theta_i} \mid h_{\text{Alice-Eve}}e^{j\theta_k}) \\ &+ \text{h}(h_{\text{Bob-Alice}}e^{j\theta_j} \mid h_{\text{Alice-Eve}}e^{j\theta_k}) \\ &- \text{h}(h_{\text{ALice-Bob}}e^{j\theta_i}, h_{\text{Bob-Alice}}e^{j\theta_j}, h_{\text{Alice-Eve}}e^{j\theta_k}) \\ &+ \text{h}(h_{\text{Alice-Eve}}e^{j\theta_k}). \end{aligned} \tag{32}$$

where h(.) is the differential entropy. The downlink channel term, $\text{h}(h_{\text{ALice-Bob}}e^{j\theta_i} \mid h_{\text{Alice-Eve}}e^{j\theta_k})$, in comparison to the direct channel quantization approach, $\text{h}(h_{\text{ALice-Bob}} \mid h_{\text{Alice-Eve}})$, offers higher equivocation of secret key bits since it holds two possibilities when applying the detection algorithm to cancel the additive phase shift at the receiver's side, Bob, as

$$\text{h}(h_{\text{ALice-Bob}}e^{j\theta_i}e^{-j\theta_i} \mid h_{\text{Alice-Eve}}e^{j\theta_k}e^{-j\theta_i})$$

$$= \text{h}(h_{\text{ALice-Bob}} \mid h_{\text{Alice-Eve}}e^{j(\theta_k-\theta_i)}) \tag{33}$$

$$> \text{h}(h_{\text{ALice-Bob}} \mid h_{\text{Alice-Eve}}). \tag{34}$$

If $k \neq i$, the term $e^{j(\theta_k-\theta_i)}$ is practically an additive noise the will degrade significantly the adversary channel detection. The passive attack is reduced to minimum and requires highly correlated channel, i.e. Eve has a very small displacement from Bob, in order to replicate the phase shift indexing. Hence, this proves the theoretical surpassing secrecy performance of our proposed algorithm that will lead to small leakage in secret key bits as will be shown later as vulnerable bits.

V. Simulation Results

We assess the performance of the proposed techniques by using a Monte Carlo simulation to examine the RSM and the RPS algorithms in order to serve two security aspects on the physical layer. Table I shows the simulation setup that is commonly used in the Long Term Evolution (LTE) [35], [36].

TABLE I
Simulation Setup.

Channel model	SCME, Vehicular A
Antenna system	Multiple antenna, single user
Modulation	QPSK, 8PSK, 16QAM
Fading	Small scale Rayleigh fading
Centre frequency	1.8/2 GHz (UL/DL)
Key length	128 bits

A. Proposed Algorithm Performance

Firstly, we illustrate the KER performance of the RSM algorithm in Fig. 10, with a multiple sub-regions, $P = 4$, as Alice is equipped with 2 transmit antennas, 2 OFDM subcarriers, and single antenna for Bob in comparison to previous work using the following approaches: Channel Quantization Approach (CQA) [12], MIMO-OFDM Physical-layer Rotated reference technique (MOPRO) [15], MIMO Precoding (MP) [27], and Phase Randomization (PR) [28]. On one hand, we can notice the superior KER performance of the proposed RSM method compared to others. On the other hand, the effect of the modulation constellation shows that with small Euclidean distances between the modulated symbols the KER performance will be degraded due to high probability of adjacent symbols interference on the constellation map. Moreover, in addition to the modulation complexity, the RSM algorithm requires low computational burden, since it needs only a sorting algorithm and look up tables meanwhile the other benchmarks requires more computations for channel decomposition and matrix multiplications which bring significant complexity as illustrated in Table II.

B. Secret Key Passive Attack

During Eve's passive attack scenario, in Section II-B1, the proposed algorithm performance is shown in Fig. 11. It is clear that the number of the vulnerable bits is dramatically reduced than other methods due to the channel gain rapid change with the change of the correlation coefficient, in other words the channel changes with small position displacement in high frequency band. Also as expected the smaller Euclidean distances between the modulated symbols the lower advantage at Eve's side that drives her deep into the uncertainty region of the constellation distribution.

TABLE II
PROCESSING COMPLEXITY OF $N_R \times N_T$ MIMO SYSTEM.

	Proposed RSM	PR	MP	MOPRO	CQA
Main Approach	Random Constellation Symbol Mapping	Randomized OFDM Symbol	Random Private MIMO Precoding	MIMO Precoding	Channel Quantization
Sorting Algorithm	$N_T \log(N_T)$	$L_{\mathcal{B}} \log(L_{\mathcal{B}})$	$L_{\mathcal{F}} \log(L_{\mathcal{F}})$	N/A	N/A
Channel Decomposition (per transmission)	N/A	N/A	N/A	$4N_R N_T^2$	$\frac{128(N_R N_T)^3}{(N_R N_T)^3+2}$
Multiplication and Modular Reduction	$2N_T$ only for RPS authentication	$2^{p+1}R$	$2^{p+1}(N_R N_T)$	$2N_T N_R^2 + 2^{p+1}(N_R+1)$	$2N_R N_T(5N_R+1)$
Look-Up-Tables	A	A	A	N/A	N/A

$L_{\mathcal{B}}$: length of phase randomization vector, $L_{\mathcal{F}}$: length of precoding matrices, R: Number of OFDM subcarriers, p: number of index bits for the randomization vector or precoding codebook, N/A: not applicable, and A: applicable.

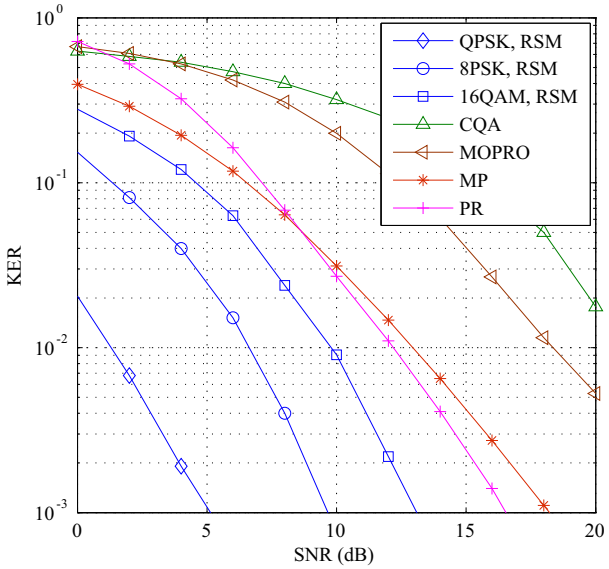

Fig. 10. Key error rate of the RSM algorithm with different types of digital modulation versus other previous works.

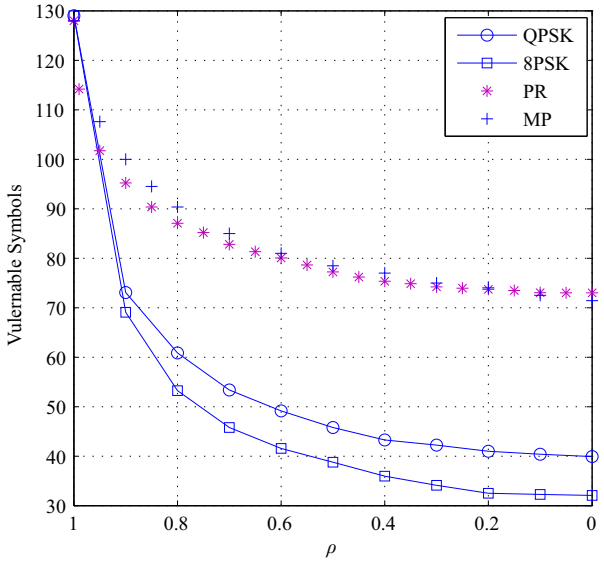

Fig. 11. Eve's correct secret key detection with her passive attack.

It is worth mentioning that although there is a number of vulnerable bits that represent the average leakage in the secret key at the adversary side but the adversary is considered incapable of finding the correct indexing of these bits and unable to enhance his attack strategy. Hence an eavesdropper in practice will follow the conventional brute force attack by applying different bits combinations at the received encrypted messages to decipher the contents of the original message. In this case it is more practical to assume that the length of the secret key is known at Eve's side and thus the length of the secret bits is considered a critical player as the longer secret key bits the more bit combination possibilities. Nowadays, secret keys of the length more than 256 bits with the Advance Encryption Standard (AES) algorithm (symmetric secret key algorithm) satisfy the security recommended requirements for secure point-to-point data exchange [1].

C. Secret key Active Attack

In order to evaluate Eve's active attack, we measure the RPS performance using two early defined metrics, the FA and the MD rates. In Fig. 12 we simulate our authentication scheme to show the uncorrelated relation between the FA and MD rates as we stated early in this paper. However, it is clear that the effect of the window width, W, improves the FA probability rate as it gets wider since each antenna has wider space that can reduce the noise effect at the receiver between the modulated symbols allocated at the same region. On the other hand, the larger window sizes can affect the KER performance since the modulated symbols may interfere with the adjacent region due to the additive noise. The other advantage of our proposed RPS algorithm is the difference of the SNR_D ($\text{SNR}_{AB} - \text{SNR}^{\text{Passive, } AE}_{\text{Active, } EB}$ in dB, lead or lag) from Alice and Eve towards Bob has no effect of the overall FA rate.

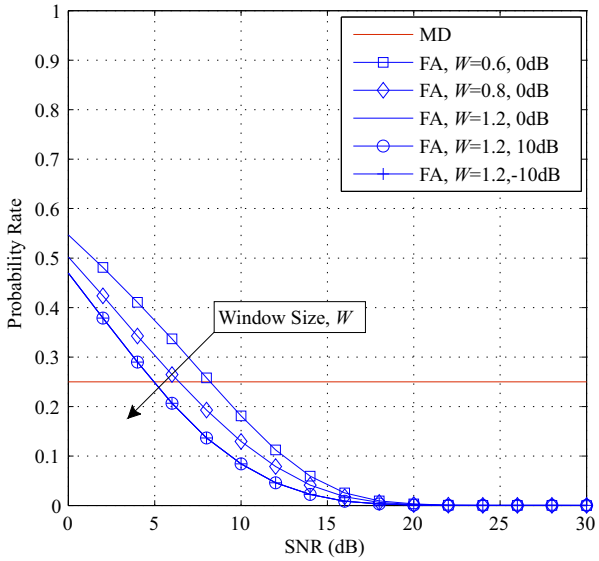

Fig. 12. MD and FA rates with respect to the SNR and (1) different window sizes, W in radian, (2) variable SNR_D, and (3) $P = 4$.

As shown in the aforementioned figure, the MD rates are constant with respect to the SNR values, meanwhile, it is very sensitive to the correlation between the channels $\mathbf{H}_{AB}$ and $\mathbf{H}_{EB}$ in the active attack scenario in Fig. 13. Despite that, it converges to its optimum value at a correlation criteria close to $\rho = 0.5$ and may proceed with this convergence proportionally with the increment of the multiples of P that results from higher orders of both antenna and frequency subcarriers. Finally, in both cases the FA and MD rates are independent of the SNR values available at the eavesdropper's side and hence it inherits the location free concept for both Alice and Bob.

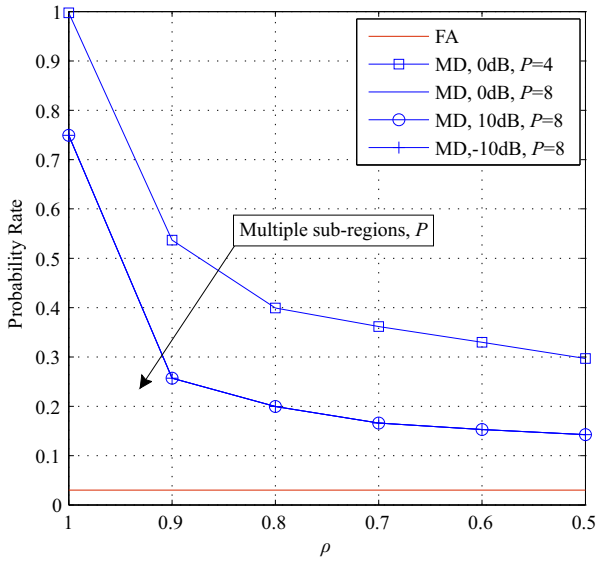

Fig. 13. MD and FA rates with respect to the correlation, window sizes (W=0.6 rad), and different SNR_D.

VI. Conclusion

This paper presented two low-complexity methods to provide physical layer based secret key exchange and authentication. The simulation results for both proposed methods have shown a superior KER performance over well-known benchmark techniques. Moreover, the secret key bits transmission is associated with authentication processing of relatively negligible FA values at medium and high SNR values. Furthermore, it was demonstrated that the proposed algorithms provide less vulnerable bits and lower MD rates with higher orders of antennas and subcarriers per receiver making these techniques potential candidates in MIMO systems.

Appendix A
Symbol Error Rate

Proof: Assume a coherent QPSK receiver with carrier signal

$$c(t) = \cos\,(2\pi f_c t + \epsilon). \tag{35}$$

where ϵ is the phase error which we assumed to be very low. Equation (19) can be written in another form after applying the sum-difference formulas of the trigonometric identities, [37], as

$$y_i(t) = \sqrt{E_s}\left(\underbrace{\sqrt{\frac{2}{T_s}}\cos\,(2\pi f_c t)}_{c_I(t)}\underbrace{\cos\,(\omega_i)}_{\alpha} - \underbrace{\sqrt{\frac{2}{T_s}}\sin\,(2\pi f_c t)}_{c_Q(t)}\underbrace{\sin\,(\omega_i)}_{\beta}\right) \tag{36}$$

Using the carrier phase estimation at the receiver, then from (36) we can see that $c_I(t)$ and $c_Q(t)$ are two quadrature carriers and orthonormal to each other [37]. Thus, α and β are sample values which decides the location of the QPSK symbol.

The form of the QPSK signal with the proposed RPS algorithm, i.e with a random phase shift (θ_i), of the symbols located at the first quarter of the complex plane, is given by

$$\tilde{y}_i(t) = \sqrt{\frac{2E_s}{T_s}}\cos\,(2\pi f_c t + \frac{\pi}{4} + \theta_i) + n(t), \tag{37}$$

$$\text{for } i = 1, 2, \tag{38}$$

where N is a white Gaussian noise with $\mathcal{CN}(0, N_0)$ distribution and is the extra perturbation that scatters the symbol around its original position. Thus the receiver has to derive the position formula for the phase detection. Hence, the two samples are

$$\alpha = \sqrt{\frac{E_s}{2}}\,(\cos\,\theta_i - \sin\theta_i), \tag{39}$$

and

$$\beta = \sqrt{\frac{E_s}{2}}\,(\cos\,\theta_i + \sin\,\theta_i). \tag{40}$$

In order to evaluate the symbol error rate, we have to find the probability that the symbol lies in the first quarter, as shown in Fig. 14,

$$\begin{aligned} P_s &= 1 - P_{(\text{symbol is in the first quarter})}, && (41)\\ &= 1 - P_{\alpha \text{ and } \beta \text{ are in the } 1^{st}\text{quarter}}, && (42)\\ &= 1 - (P_\alpha \times P_\beta)\,. && (43) \end{aligned}$$

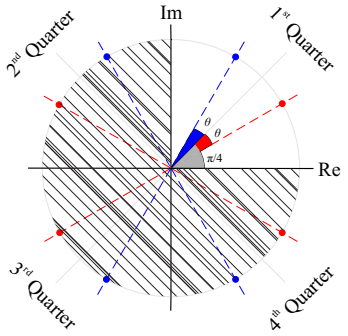

Fig. 14. The proposed RPS-QPSK Constellation with 1×2 MISO system where $\theta_1 = \theta_{\text{Ant.1}}$ and $\theta_2 = \theta_{\text{Ant.2}}$.

$$\begin{aligned} P_\alpha &= \frac{1}{\sqrt{\pi N_0}} \int_0^\infty e^{-\frac{\left(\alpha - \sqrt{\frac{E_s}{2}}\,(\cos\,\theta_i - \sin\theta_i)\right)^2}{N_0}} d\alpha, && (44)\\ &= 1 - \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_i - \sin\,\theta_i)\right), && (45) \end{aligned}$$

and

$$\begin{aligned} P_\beta &= \frac{1}{\sqrt{\pi N_0}} \int_0^\infty e^{-\frac{\left(\beta - \sqrt{\frac{E_s}{2}}\,(\cos\,\theta_i + \sin\theta_i)\right)^2}{N_0}} d\beta, && (46)\\ &= 1 - \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_i + \sin\,\theta_i)\right), && (47) \end{aligned}$$

where,

$$\text{erfc}\,(x) = \frac{2}{\sqrt{\pi}} \int_x^\infty e^{-u^2} du. \tag{48}$$

Thus, combining the results in (45 and 47) and substitute it in 43 yields

$$\begin{aligned} P_s &\simeq \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_i - \sin\,\theta_i)\right) && (49)\\ &+ \frac{1}{2}\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_i + \sin\,\theta_i)\right), && (50) \end{aligned}$$

■

Appendix B
Phase Error Rate

In this section we can use the same method in Appendix A, but for the sake of clarity and ease of derivation for Corollary 3 we will use the same approximation method used in (Theorem 6.10.1, [38]).

Proof: For any random symbol lies in any of the four quarter, compute the minimum distance $d_{\min}$ which separates the symbol from joint symbols. Consider the constellation diagram in Fig. 15 then find $d_{\min 1}$, $d_{\min 2}$ and $d_{\min 3}$ for the symbols sharing the same antenna zone. Therefore,

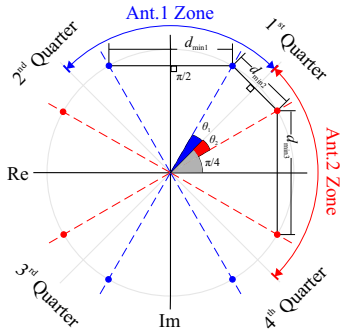

Fig. 15. The proposed RPS-QPSK constellation and antenna zones with 1×2 MISO system.

$$P_p = P_1 P_{e|1} + P_2 P_{e|2}, \tag{51}$$

$$\begin{aligned} d_{\min 1} &= 2\sqrt{\frac{E_s}{2}}\,\cos\,\theta_1, && (52)\\ d_{\min 2} &= \sqrt{E_s}\,\sin\,\theta_1 + \sqrt{E_s}\,\sin\,\theta_2, && (53)\\ d_{\min 3} &= 2\sqrt{\frac{E_s}{2}}\,\cos\,\theta_2. && (54) \end{aligned}$$

Using Theorem 6.10.1 mentioned above, then

$$\begin{aligned} P_{e|1} &= \frac{1}{2}\left(\text{erfc}\left(\frac{d_{\min 1}}{2\sqrt{2}\sigma}\right) + \text{erfc}\left(\frac{d_{\min 2}}{2\sqrt{2}\sigma}\right)\right), && (55)\\ P_{e|2} &= \frac{1}{2}\left(\text{erfc}\left(\frac{d_{\min 3}}{2\sqrt{2}\sigma}\right) + \text{erfc}\left(\frac{d_{\min 2}}{2\sqrt{2}\sigma}\right)\right), && (56) \end{aligned}$$

where σ is the noise variance, such that for a white Gaussian noise distribution $\sigma = \sqrt{N_0/2}$. Substitute equations (52-56) in (51) and neglect the small terms for the high SNR case, yields the phase error rate of the shift detection as

$$\begin{aligned} P_p &\simeq \frac{1}{4}\left[\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_1)\right)\right.\\ &+ \left.\,\text{erfc}\left(\sqrt{\frac{E_s}{2N_0}}\,(\cos\,\theta_2)\right)\right]\\ &+ \frac{1}{2}\left[\,\text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,(\sin\,\theta_1)\right)\right.\\ &+ \left.\,\text{erfc}\left(\frac{1}{2}\sqrt{\frac{E_s}{N_0}}\,(\sin\,\theta_2)\right)\right] && (57) \end{aligned}$$

■

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principle and Practice*, 6th ed. Pearson, 2014.

[2] C.E.Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656–715, April 1949.

[3] A. Wyner, "The Wire-tap Channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[4] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian Wiretap Channel," *IEEE Transaction on Information Theory*, vol. 24, no. 4, pp. 451–456, 1978.

[5] S. Liu, Y. Hong, and E. Viterbo, "Unshared Secret Key Cryptography," *IEEE Transactions on Wireless Communications*, vol. 13, no. 12, pp. 6670–6683, Dec 2014.

[6] F. Zhu, F. Gao, M. Yao, and H. Zou, "Joint Information and Jamming Beamforming for Physical Layer Security With Full Duplex Base Station," *IEEE Transactions on Signal Processing*, vol. 62, no. 24, pp. 6391–6401, Dec 2014.

[7] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced Secrecy in Stochastic Wireless Networks: Artificial Noise With Secrecy Protected Zone," *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 10, pp. 1617–1628, Oct 2014.

[8] B. Quist and M. Jensen, "Bound on the Key Establishment Rate for Multi-Antenna Reciprocal Electromagnetic Channels," *Antennas and Propagation, IEEE Transactions on*, vol. 62, no. 3, pp. 1378–1385, March 2014.

[9] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 2593–2597.

[10] N. Patwari, J. Croft, S. Jana, and S. Kasera, "High-Rate Uncorrelated Bit Extraction for Shared Secret Key Generation from Channel Measurements," *Mobile Computing, IEEE Transactions on*, vol. 9, no. 1, pp. 17–30, Jan 2010.

[11] A. Sayeed and A. Perrig, "Secure Wireless Communications: Secret Keys Through Multipath," in *Acoustics, Speech and Signal Processing, 2008. ICASSP 2008. IEEE International Conference on*, March 2008, pp. 3013–3016.

[12] C. Chen and M. Jensen, "Secret Key Establishment Using Temporally and Spatially Correlated Wireless Channel Coefficients," *Mobile Computing, IEEE Transactions on*, vol. 10, no. 2, pp. 205–215, Feb 2011.

[13] K. Zeng, D. Wu, A. Chan, and P. Mohapatra, "Exploiting Multiple-Antenna Diversity for Shared Secret Key Generation in Wireless Networks," in *INFOCOM, 2010 Proceedings IEEE*, March 2010, pp. 1–9.

[14] J. W. Wallace and R. K. Sharma, "Automatic Secret Keys From Reciprocal MIMO Wireless Channels: Measurement and Analysis," *IEEE Transaction on Information Forensics and Security*, vol. 5, no. 3, pp. 381–392, Sept. 2010.

[15] P.-C. Y. C.-H. L. Chih-Yao Wu, Pang-Chang Lan and C.-M. Cheng, "Practical Physical Layer Security Schemes for MIMO-OFDM Systems Using Precoding Matrix Indices," *IEEE journal on selected areas in communications*, vol. 31, no. 9, pp. 1687–1700, Sept. 2013.

[16] B. Zan, M. Gruteser, and F. Hu, "Key Agreement Algorithms for Vehicular Communication Networks Based on Reciprocity and Diversity Theorems," *Vehicular Technology, IEEE Transactions on*, vol. 62, no. 8, pp. 4020–4027, Oct 2013.

[17] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad Hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, April 2016.

[18] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel-Based Spoofing Detection in Frequency-Selective Rayleigh Channels," *IEEE Transactions on Wireless Communications*, vol. 8, no. 12, pp. 5948–5956, December 2009.

[19] J. K. Tugnait, "Wireless User Authentication via Comparison of Power Spectral Densities," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 1791–1802, September 2013.

[20] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Using the Physical Layer for Wireless Authentication in Time-Variant Channels," *IEEE Transactions on Wireless Communications*, vol. 7, no. 7, pp. 2571–2579, July 2008.

[21] F. J. Liu, X. Wang, and S. L. Primak, "A Two Dimensional Quantization Algorithm for CIR-Based Physical Layer Authentication," in *Communications (ICC), 2013 IEEE International Conference on*, June 2013, pp. 4724–4728.

[22] E. Jorswieck, S. Tomasin, and A. Sezgin, "Broadcasting into the Uncertainty: Authentication and Confidentiality by Physical-Layer Processing," *Proceedings of the IEEE*, vol. 103, no. 10, pp. 1702–1724, Oct 2015.

[23] M. D. Renzo and H. Haas, "Bit Error Probability of SM-MIMO Over Generalized Fading Channels," *IEEE Transactions on Vehicular Technology*, vol. 61, no. 3, pp. 1124–1144, March 2012.

[24] C. Masouros, "Improving the Diversity of Spatial Modulation in MISO Channels by Phase Alignment," *IEEE Communications Letters*, vol. 18, no. 5, pp. 729–732, May 2014.

[25] C. Masouros and L. Hanzo, "Constellation Randomization Achieves Transmit Diversity for Single-RF Spatial Modulation," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 10, pp. 8101–8111, Oct 2016.

[26] ——, "A Scalable Performance-Complexity Tradeoff for Constellation Randomization in Spatial Modulation," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 3, pp. 2834–2838, March 2017.

[27] H. Taha and E. Alsusa, "Secret Key Exchange using Private Random Precoding in MIMO FDD and TDD Systems," *IEEE Transactions on Vehicular Technology*, vol. PP, no. 99, pp. 1–1, October 2016.

[28] ——, "Secret Key Establishment Technique Using Channel State Information Driven Phase Randomisation in Multiple-Input Multiple-Output Orthogonal Frequency Division Multiplexing," *IET Information Security*, vol. 11, no. 1, pp. 1–7, January 2017.

[29] M. D. Renzo, H. Haas, and P. M. Grant, "Spatial Modulation for Multiple-Antenna Wireless Systems: a Survey," *IEEE Communications Magazine*, vol. 49, no. 12, pp. 182–191, December 2011.

[30] N. Ferdinand, D. da Costa, A. de Almeida, and M. Latva-aho, "Physical Layer Secrecy Performance of TAS Wiretap Channels with Correlated Main and Eavesdropper Channels," *Wireless Communications Letters, IEEE*, vol. 3, no. 1, pp. 86–89, February 2014.

[31] T.-H. Chou, S. Draper, and A. Sayeed, "Secret Key Generation from Sparse Wireless Channels: Ergodic Capacity and Secrecy Outage," *Selected Areas in Communications, IEEE Journal on*, vol. 31, no. 9, pp. 1751–1764, September 2013.

[32] J. Boutros and E. Viterbo, "Signal Space Diversity: a Power- and Bandwidth-Efficient Diversity Technique for the Rayleigh Fading Channel," *IEEE Transactions on Information Theory*, vol. 44, no. 4, pp. 1453–1467, Jul 1998.

[33] M. Hayashi and T. Tsurumaru, "More Efficient Privacy Amplification With Less Random Seeds via Dual Universal Hash Function," *IEEE Transactions on Information Theory*, vol. 62, no. 4, pp. 2213–2232, April 2016.

[34] C. Ye, A. Reznik, and Y. Shah, "Extracting Secrecy from Jointly Gaussian Random Variables," in *Information Theory, 2006 IEEE International Symposium on*, July 2006, pp. 2593–2597.

[35] 3GPP, "Spatial Channel Model for Multiple Input Multiple Output (MIMO) Simulations, Version 12.0.0 Release 12," 3rd Generation Partnership Project (3GPP), TR 25.996, Sep. 2014.

[36] 3GPP, "Measurement of Radiated Performance for Multiple Input Multiple Output (MIMO) and Multi-Antenna Reception for High Speed Packet Access (HSPA) and LTE Terminals, Version 12.0.0 Release 12," 3rd Generation Partnership Project (3GPP), TR 37.976, Oct. 2014.

[37] J. Proakis and M. Salehi, *Digital Communications*, ser. McGraw-Hill International Edition. McGraw-Hill, 2008.

[38] R. Blahut, *Modem Theory: An Introduction to Telecommunications*, ser. Modem Theory: An Introduction to Telecommunications. Cambridge University Press, 2010.